

Partial permutation decoding for binary linear and \mathbb{Z}_4 -linear Hadamard codes ^{*}

Roland D. Barrolleta[†] Mercè Villanueva[†]

May 3, 2016

Abstract

Permutation decoding is a technique which involves finding a subset S , called PD-set, of the permutation automorphism group of a code C in order to assist in decoding. An explicit construction of $\left\lfloor \frac{2^m - m - 1}{1 + m} \right\rfloor$ -PD-sets of minimum size $\left\lfloor \frac{2^m - m - 1}{1 + m} \right\rfloor + 1$ for partial permutation decoding for binary linear Hadamard codes H_m of length 2^m , for all $m \geq 4$, is described. Moreover, a recursive construction to obtain s -PD-sets of size l for H_{m+1} of length 2^{m+1} , from a given s -PD-set of the same size for H_m , is also established. These results are generalized to find s -PD-sets for (nonlinear) binary Hadamard codes of length 2^m , called \mathbb{Z}_4 -linear Hadamard codes, which are obtained as the Gray map image of quaternary linear codes of length 2^{m-1} .

Index terms— automorphism group, permutation decoding, PD-set, Hadamard code, \mathbb{Z}_4 -linear code

1 Introduction

Denote by \mathbb{Z}_2 and \mathbb{Z}_4 the rings of integers modulo 2 and modulo 4, respectively. Let \mathbb{Z}_2^n denote the set of all binary vectors of length n and let \mathbb{Z}_4^n be the set of all n -tuples over the ring \mathbb{Z}_4 . The *Hamming weight* $\text{wt}(v)$ of a vector $v \in \mathbb{Z}_2^n$ is the number of nonzero coordinates in v . The *Hamming distance* $d(u, v)$ between two vectors $u, v \in \mathbb{Z}_2^n$ is the number of coordinates in which u and v differ, that is, $d(u, v) = \text{wt}(u + v)$. Let e_i be the binary vector or tuple over \mathbb{Z}_4 with a one in the i th coordinate and zeros elsewhere. Let **0**, **1**, **2** and **3** be the binary vectors or tuples over \mathbb{Z}_4 having 0, 1, 2 and 3, respectively, repeated in each coordinate. It will be clear by the context whether we refer to binary vectors or tuples over \mathbb{Z}_4 .

Any nonempty subset C of \mathbb{Z}_2^n is a binary code and a subgroup of \mathbb{Z}_2^n is called a *binary linear code*. Equivalently, any nonempty subset \mathcal{C} of \mathbb{Z}_4^n is a quaternary

^{*}This work was partially supported by the Spanish MINECO under Grant TIN2013-40524-P, and by the Catalan AGAUR under Grant 2014SGR-691. The material in this paper was presented in part at IX “Jornadas de Matemática Discreta y Algorítmica” in Tarragona, Spain, 2014 [1].

[†]Departament d’Enginyeria de la Informació i de les Comunicacions, Universitat Autònoma de Barcelona, e-mails: rolanddavid.barrolleta@uab.cat and merce.villanueva@uab.cat.

code and a subgroup of \mathbb{Z}_4^n is called a *quaternary linear code*. Quaternary codes can be seen as binary codes under the usual Gray map $\Phi : \mathbb{Z}_4^n \rightarrow \mathbb{Z}_2^{2n}$ defined as $\Phi((y_1, \dots, y_n)) = (\phi(y_1), \dots, \phi(y_n))$, where $\phi(0) = (0, 0)$, $\phi(1) = (0, 1)$, $\phi(2) = (1, 1)$, $\phi(3) = (1, 0)$, for all $y = (y_1, \dots, y_n) \in \mathbb{Z}_4^n$. If \mathcal{C} is a quaternary linear code, the binary code $C = \Phi(\mathcal{C})$ is said to be a \mathbb{Z}_4 -linear code. Moreover, since \mathcal{C} is a subgroup of \mathbb{Z}_4^n , it is isomorphic to an abelian group $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ and we say that \mathcal{C} (or equivalently the corresponding \mathbb{Z}_4 -linear code $C = \Phi(\mathcal{C})$) is of type $2^\gamma 4^\delta$ [7].

Let C be a binary code of length n and size $|C| = 2^k$. For a vector $v \in \mathbb{Z}_2^n$ and a set $I \subseteq \{1, \dots, n\}$, we denote by v_I the restriction of v to the coordinates in I and by C_I the set $\{v_I : v \in C\}$. A set $I \subseteq \{1, \dots, n\}$ of k coordinate positions is an *information set* for C if $|C_I| = 2^k$. If such an I exists, C is said to be a *systematic code*. For each information set I of size k , the set $\{1, \dots, n\} \setminus I$ of the remaining $n - k$ coordinate positions is a *check set* for C .

Let $\text{Sym}(n)$ be the symmetric group of permutations on the set $\{1, \dots, n\}$ and let $\text{id} \in \text{Sym}(n)$ be the identity permutation. The group operation in $\text{Sym}(n)$ is the function composition $\sigma_1 \sigma_2$, which maps any element x to $\sigma_1(\sigma_2(x))$, $\sigma_1, \sigma_2 \in \text{Sym}(n)$. A $\sigma \in \text{Sym}(n)$ acts linearly on words of \mathbb{Z}_2^n or \mathbb{Z}_4^n by permuting their coordinates as follows: $\sigma((v_1, \dots, v_n)) = (v_{\sigma^{-1}(1)}, \dots, v_{\sigma^{-1}(n)})$. The *permutation automorphism group* of \mathcal{C} or $C = \Phi(\mathcal{C})$, denoted by $\text{PAut}(\mathcal{C})$ or $\text{PAut}(C)$, respectively, is the group generated by all permutations that preserve the set of codewords.

A *binary Hadamard code* of length n has $2n$ codewords and minimum distance $n/2$. It is well-known that there exists a unique binary linear Hadamard code H_m of length $n = 2^m$, for any $m \geq 2$. The quaternary linear codes such that, under the Gray map, give a binary Hadamard code are called *quaternary linear Hadamard codes* and the corresponding \mathbb{Z}_4 -linear codes are called *\mathbb{Z}_4 -linear Hadamard codes*. These codes have been studied and classified in [10, 13], and their permutation automorphism groups have been determined in [9, 14].

Permutation decoding is a technique, introduced in [11] by MacWilliams for linear codes, which involves finding a subset of the permutation automorphism group of a code in order to assist in decoding. A new permutation decoding method for \mathbb{Z}_4 -linear codes (not necessarily linear) was introduced in [2]. In general, the method works as follows. Given a systematic t -error-correcting code C with information set I , we denote by $y = x + e$ the received vector, where $x \in C$ and e is the error vector. Suppose that at most t errors occur, that is, $\text{wt}(e) \leq t$. The permutation decoding consists on moving all errors in y out of I , by using an automorphism of C . This technique is strongly based on the existence of some special subsets of $\text{PAut}(C)$, called PD-sets. Specifically, a subset $S \subseteq \text{PAut}(C)$ is said to be an s -PD-set for the code C if every s -set of coordinate positions is moved out of I by at least one element of S , where $1 \leq s \leq t$. When $s = t$, S is said to be a PD-set.

In [4], it is shown how to find s -PD-sets of size $s + 1$ that satisfy the Gordon-Schönheim bound for partial permutation decoding for the binary simplex code of length $2^m - 1$ for all $m \geq 4$ and $1 < s \leq \lfloor \frac{2^m - m - 1}{m} \rfloor$. In this paper, following the same technique, similar results for binary linear and \mathbb{Z}_4 -linear Hadamard codes are established. In [15], 2-PD-sets of size 5 and 4-PD-sets of size $\binom{m+1}{2} + 2$ are found for binary linear Hadamard codes H_m , for all $m > 4$. Small PD-sets that satisfy the Gordon-Schönheim bound have also been found for binary

Golay codes [5, 16] and for the binary simplex code S_4 [8].

This work is organized as follows. In Section 2, we prove that the Gordon-Schönheim bound can be adapted to systematic codes, not necessarily linear. Furthermore, we apply this bound on the minimum size of s -PD-sets to binary linear and \mathbb{Z}_4 -linear Hadamard codes, which are systematic but nonlinear in general, and we prove that their minimum size is $s + 1$. In Section 3, we regard the permutation automorphism group $\text{PAut}(H_m)$ as a certain subgroup of the general linear group $\text{GL}(m + 1, 2)$ and we provide a criterion on subsets of matrices of such subgroup to be an s -PD-set of size $s + 1$ for H_m . In Section 4, we define recursive constructions to obtain s -PD-sets of size l for H_{m+1} from a given s -PD-set of the same size for H_m , where $l \geq s + 1$. Finally, in Sections 5 and 6, we establish equivalent results for (nonlinear) \mathbb{Z}_4 -linear Hadamard codes.

2 Minimum size of s -PD-sets for Hadamard codes

There is a well-known bound on the minimum size of PD-sets for linear codes based on the length, dimension and minimum distance of such codes that can be adapted to systematic codes (not necessarily linear) easily.

Proposition 1. *Let C be a systematic t -error correcting code of length n , size $|C| = 2^k$ and minimum distance d . Let $r = n - k$ be the redundancy of C . If S is a PD-set for C , then*

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil. \quad (1)$$

The above inequality (1) is often called the *Gordon-Schönheim bound*. The result given by Proposition 1 is quoted and proved for linear codes in [6]. We can follow the same proof, since the linearity of the code is only used to guarantee that the code is systematic. In [2], it is shown that \mathbb{Z}_4 -linear codes are systematic, and a systematic encoding is given for these codes. Therefore, the result can be applied to any \mathbb{Z}_4 -linear code, not necessarily linear.

The Gordon-Schönheim bound can be adapted to s -PD-sets for all s up to the error correcting capability of the code. Note that the error-correcting capability of any binary linear or \mathbb{Z}_4 -linear Hadamard code of length $n = 2^m$ is $t_m = \lfloor (d-1)/2 \rfloor = \lfloor (2^{m-1}-1)/2 \rfloor = 2^{m-2} - 1$ [12]. Moreover, all these codes are systematic and have size $2n = 2^{m+1}$. Therefore, the right side of the bound given by (1), for binary linear and \mathbb{Z}_4 -linear Hadamard codes of length 2^m and for all $1 \leq s \leq t_m$, becomes

$$g_m(s) = \left\lceil \frac{2^m}{2^m - m - 1} \left\lceil \frac{2^m - 1}{2^m - m - 2} \left\lceil \cdots \left\lceil \frac{2^m - s + 1}{2^m - m - s} \right\rceil \cdots \right\rceil \right\rceil \right\rceil. \quad (2)$$

We compute the minimum value of $g_m(s)$ in the following lemma.

Lemma 2. *Let m be an integer, $m \geq 4$. For $1 \leq s \leq t_m$,*

$$g_m(s) = \left\lceil \frac{2^m}{2^m - m - 1} \left\lceil \frac{2^m - 1}{2^m - m - 2} \left\lceil \cdots \left\lceil \frac{2^m - s + 1}{2^m - m - s} \right\rceil \cdots \right\rceil \right\rceil \right\rceil \geq s + 1,$$

where $t_m = 2^{m-2} - 1$ is the error-correcting capability of any binary linear and \mathbb{Z}_4 -linear Hadamard code of length 2^m .

Proof. We need to prove that $g_m(s) \geq s + 1$. This fact is clear, since the central term

$$\left\lceil \frac{2^m - s + 1}{2^m - m - s} \right\rceil = 2$$

for all $s \in \{1, \dots, 2^{m-2} - 1\}$, and in each stage of the ceiling function working from inside, $g_m(s)$ increases its value by at least 1. \square

The smaller the size of the PD-set is, the more efficient permutation decoding becomes. Because of this, we will focus on the case when we have that $g_m(s) = s + 1$. For each binary linear and \mathbb{Z}_4 -linear Hadamard code of length 2^m , $m \geq 4$, we define the following integer:

$$f_m = \max\{s : 2 \leq s, g_m(s) = s + 1\},$$

which represents the greater s in which we can find s -PD-sets of size $s + 1$. The following result characterizes this parameter from the value of m . Note that for $m = 3$, since the error-correcting capability is $t_3 = 1$, the permutation decoding becomes unnecessary and we do not take it into account in the results.

Lemma 3. *Let m be an integer, $m \geq 4$. Then, $f_m = \left\lfloor \frac{2^m - m - 1}{1 + m} \right\rfloor$.*

Proof. The result is easy to prove by Lemma 2 and following a similar argument as the one in the proof of Lemma 2 in [4]. \square

3 Finding s -PD-sets of size $s + 1$ for binary linear Hadamard codes

For any $m \geq 2$, there is a unique binary linear Hadamard code H_m of length 2^m [12]. A generator matrix G_m for H_m can be constructed as follows:

$$G_m = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{0} & G' \end{pmatrix}, \quad (3)$$

where G' is any matrix having as column vectors the $2^m - 1$ nonzero vectors from \mathbb{Z}_2^m , with the vectors e_i , $i \in \{1, \dots, m\}$, in the first m positions. Note that G' can be seen as a generator matrix of the binary simplex code of length $2^m - 1$.

By construction, from (3), it is clear that $I_m = \{1, \dots, m + 1\}$ is an information set for H_m . Let w_i be the i th column vector of G_m , $i \in \{1, \dots, 2^m\}$. By labelling the coordinate positions with the columns of G_m , we can take as an information set I_m for H_m the first $m + 1$ column vectors of G_m considered as row vectors, that is, $I_m = \{w_1, \dots, w_{m+1}\} = \{e_1, e_1 + e_2, \dots, e_1 + e_{m+1}\}$. Then, depending on the context, I_m will be taken as a subset of $\{1, \dots, 2^m\}$ or as a subset of $\{1\} \times \mathbb{Z}_2^m$.

Example 4. *Let H_4 be the binary linear Hadamard code of length 16 with generator matrix*

$$G_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad (4)$$

constructed as in (3). The set $I_4 = \{1, 2, 3, 4, 5\}$, or equivalently the set of column vectors $I_4 = \{w_1, w_2, w_3, w_4, w_5\} = \{e_1, e_1 + e_2, e_1 + e_3, e_1 + e_4, e_1 + e_5\}$ of G_4 , is an information set for H_4 .

It is known that the permutation automorphism group $\text{PAut}(H_m)$ of H_m is isomorphic to the general affine group $\text{AGL}(m, 2)$ [12]. Let $\text{GL}(m, 2)$ be the general linear group over \mathbb{Z}_2 . Recall that $\text{AGL}(m, 2)$ consists of all mappings $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$ of the form $\alpha(x) = Ax + b$ for $x \in \mathbb{Z}_2^m$, where $A \in \text{GL}(m, 2)$ and $b \in \mathbb{Z}_2^m$, together with the function composition as the group operation. The monomorphism

$$\begin{aligned} \varphi : \text{AGL}(m, 2) &\longrightarrow \text{GL}(m+1, 2) \\ (b, A) &\longmapsto \begin{pmatrix} 1 & b \\ \mathbf{0} & A \end{pmatrix} \end{aligned}$$

defines an isomorphism between $\text{AGL}(m, 2)$ and the subgroup of $\text{GL}(m+1, 2)$ consisting of all nonsingular matrices whose first column is e_1 . Therefore, from now on, we also regard $\text{PAut}(H_m)$ as this subgroup. Note that any matrix $M \in \text{PAut}(H_m)$ can be seen as a permutation of coordinate positions, that is, as an element of $\text{Sym}(2^m)$. By multiplying each column vector w_i of G_m by M , we obtain another column vector $w_j = w_i M$, which means that the i th coordinate position moves to the j th coordinate position, $i, j \in \{1, \dots, 2^m\}$.

Let $M \in \text{PAut}(H_m)$ and let m_i be the i th row of M , $i \in \{1, \dots, m+1\}$. We define M^* as the matrix where the first row is m_1 and the i th row is $m_1 + m_i$, $i \in \{2, \dots, m+1\}$. An s -PD-set of size $s+1$ for H_m meets the Gordon-Schönheim bound if $2 \leq s \leq f_m$. The following theorem provides us a condition on sets of matrices of $\text{PAut}(H_m)$ in order to be s -PD-sets of size $s+1$ for H_m .

Theorem 5. *Let H_m be the binary linear Hadamard code of length 2^m , with $m \geq 4$. Let $P_s = \{M_i : 0 \leq i \leq s\}$ be a set of $s+1$ matrices in $\text{PAut}(H_m)$. Then, P_s is an s -PD-set of size $s+1$ for H_m with information set I_m if and only if no two matrices $(M_i^{-1})^*$ and $(M_j^{-1})^*$ for $i \neq j$ have a row in common. Moreover, any subset $P_k \subseteq P_s$ of size $k+1$ is a k -PD-set for $k \in \{1, \dots, s\}$.*

Proof. Suppose that the set $P_s = \{M_i : 0 \leq i \leq s\}$ satisfies that no two matrices $(M_i^{-1})^*$ and $(M_j^{-1})^*$ for $i \neq j$ have a row in common. Let $E = \{v_1, \dots, v_s\} \subseteq \{1\} \times \mathbb{Z}_2^m$ be a set of s different column vectors of the generator matrix G_m regarded as row vectors, which represents a set of s error positions. Assume we cannot move all the error positions to the check set by any element of P_s . Then, for each $i \in \{0, \dots, s\}$, there is a $v \in E$ such that $vM_i \in I_m$. In other words, there is at least an error position that remains in the information set I_m after applying any permutation of P_s . Note that there are $s+1$ values for i , but only s elements in E . Therefore, $vM_i \in I_m$ and $vM_j \in I_m$ for some $v \in E$ and $i \neq j$. Suppose $vM_i = w_r$ and $vM_j = w_t$, for $w_r, w_t \in I_m$. Then, $v = w_r M_i^{-1} = w_t M_j^{-1}$. Taking into account the form of the vectors in the information set $I_m = \{w_1, \dots, w_{m+1}\}$, by multiplying for such inverse matrices M_i^{-1} and M_j^{-1} , we get the first row or a certain addition between the first row and another row of each matrix. Thus, we obtain that $(M_i^{-1})^*$ and $(M_j^{-1})^*$ have a row in common, contradicting our assumption. Let $P_k \subseteq P_s$ of size $k+1$. If this set satisfies the condition on the inverse matrices and we suppose that it is not a k -PD-set, we arrive to a contradiction in the same way as before.

Conversely, suppose that the set $P_s = \{M_i : 0 \leq i \leq s\}$ forms an s -PD-set for H_m , but does not satisfy the condition on the inverse matrices. Thus, some $v \in \{w_1, \dots, w_{2^m}\}$ must be the r th row of $(M_i^{-1})^*$ and the t th row of $(M_j^{-1})^*$ for some $r, t \in \{1, \dots, m+1\}$, $i, j \in \{0, \dots, s\}$. In other words, we have that $v = e_r(M_i^{-1})^* = e_t(M_j^{-1})^*$. Therefore, $v = w_r M_i^{-1} = w_t M_j^{-1}$, where $w_r, w_t \in I_m$. Finally, we obtain that $v M_i = w_r$ and $v M_j = w_t$. These equalities implies that the vector v , which represents an error position, cannot be moved to the check set by the permutations defined by matrices M_i and M_j . Let $L = \{l : 0 \leq l \leq s, l \neq i, j\}$. For each $l \in L$, choose a row v_l of $(M_l^{-1})^*$. It is clear that $v_l = e_t(M_l^{-1})^* = w_t M_l^{-1}$, so $v_l M_l = w_t \in I_m$. Finally, since some of the v_l may repeat, we obtain a set $E = \{v_l : l \in L\} \cup \{v\}$ of size at most s . Nevertheless, no matrix in P_s will map every member of E into the check set, fact that contradicts our assumption. \square

We give now an explicit construction of an f_m -PD-set $\{M_0, \dots, M_{f_m}\} \subseteq \text{PAut}(H_m)$ of minimum size f_m+1 for the binary linear Hadamard code H_m of length 2^m . We follow a similar technique to the one described for simplex codes in [4].

Lemma 6. *Let $K = \mathbb{Z}_2[x]/(f(x))$, where $f(x)$ is a primitive polynomial of degree m . If α is a root of $f(x)$, then $\alpha^{i+1} - \alpha^i, \dots, \alpha^{i+m} - \alpha^i$ are linearly independent over \mathbb{Z}_2 , for all $i \in \{0, \dots, 2^m - 2\}$.*

Proof. It is straightforward to see that $\alpha^{i+1} - \alpha^i, \dots, \alpha^{i+m} - \alpha^i$ are linearly independent over \mathbb{Z}_2 , for all $i \in \{0, \dots, 2^m - 2\}$, if and only if $\alpha - 1, \dots, \alpha^m - 1$ are linearly independent over \mathbb{Z}_2 , since $\alpha^i \in K \setminus \{0\}$.

Note that $\alpha^m - 1 = \sum_{j=1}^{m-1} \mu_j \alpha^j$, where the sum has an odd number of nonzero terms, since $f(x)$ is irreducible. Let $\mu = (\mu_1, \dots, \mu_{m-1}) \in \mathbb{Z}_2^{m-1}$. Note that in vectorial notation $\alpha^j - 1 = e_1 + e_j$, $j \in \{1, \dots, m-1\}$ and $\alpha^m - 1 = \sum_{j=1}^{m-1} \mu_j e_{j+1}$. Finally, it is easy to see that the $m \times m$ binary matrix

$$\begin{pmatrix} 1 & \text{Id}_{m-1} \\ 0 & \mu \end{pmatrix},$$

which has as rows $\alpha - 1, \dots, \alpha^m - 1$, has determinant $\sum_{j=1}^{m-1} \mu_j = 1 \neq 0$. \square

For $i \in \{1, \dots, f_m\}$, consider the following $(m+1) \times (m+1)$ binary matrices:

$$N_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \vdots & \vdots \\ 0 & \alpha^{m-1} \end{pmatrix} \quad \text{and} \quad N_i = \begin{pmatrix} 1 & \alpha^{(m+1)i-1} \\ 0 & \alpha^{(m+1)i} - \alpha^{(m+1)i-1} \\ \vdots & \vdots \\ 0 & \alpha^{(m+1)i+m-1} - \alpha^{(m+1)i-1} \end{pmatrix}.$$

Theorem 7. *Let $P_{f_m} = \{M_i : 0 \leq i \leq f_m\}$, where $M_i = N_i^{-1}$. Then, P_{f_m} is an f_m -PD-set of size $f_m + 1$ for the binary linear Hadamard code H_m of length 2^m with information set I_m .*

Proof. Clearly, $N_0 \in \text{PAut}(H_m)$, since it is the identity matrix. By Lemma 6, $N_i \in \text{PAut}(H_m)$ for all $i \in \{1, \dots, f_m\}$. Moreover, rows of matrices $N_0^*, \dots, N_{f_m}^*$ form the set $\{(1, a) : a \in \{0, 1, \alpha, \dots, \alpha^{f_m(m+1)+m-1}\}\}$. The elements of such set are different since α is primitive and $f_m(m+1)+m-1 \leq 2^m - 2$. Theorem 5 completes the proof. \square

Example 8. Let H_4 be the binary linear Hadamard code of length 16 with generator matrix (4). Let $K = \mathbb{Z}_2[x]/(x^4 + x + 1)$ and α a root of $x^4 + x + 1$. Matrices $N_0 = \text{Id}_5$,

$$N_1 = \begin{pmatrix} 1 & \alpha^4 \\ 0 & \alpha^5 - \alpha^4 \\ 0 & \alpha^6 - \alpha^4 \\ 0 & \alpha^7 - \alpha^4 \\ 0 & \alpha^8 - \alpha^4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}, \quad N_2 = \begin{pmatrix} 1 & \alpha^9 \\ 0 & \alpha^{10} - \alpha^9 \\ 0 & \alpha^{11} - \alpha^9 \\ 0 & \alpha^{12} - \alpha^9 \\ 0 & \alpha^{13} - \alpha^9 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix},$$

where Id_5 is the 5×5 identity matrix, are elements of $\text{PAut}(H_4)$ and $P_2 = \{N_0^{-1}, N_1^{-1}, N_2^{-1}\}$ is a 2-PD-set of size 3 for H_4 . It is straightforward to check that matrices N_0^* ,

$$N_1^* = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}, \quad \text{and} \quad N_2^* = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix},$$

have no rows in common. Finally, no s -PD-set of size $s + 1$ can be found for $s \geq 3$ since $f_4 = 2$.

Let S be an s -PD-set of size $s + 1$. The set S is a *nested* s -PD-set if there is an ordering of the elements of S , $S = \{\sigma_0, \dots, \sigma_s\}$, such that $S_i = \{\sigma_0, \dots, \sigma_i\} \subseteq S$ is an i -PD-set of size $i + 1$, for all $i \in \{0, \dots, s\}$. Note that $S_i \subset S_j$ if $0 \leq i < j \leq s$ and $S_s = S$. From Theorem 5, we have two important consequences. The first one is related to how to obtain nested s -PD-sets and the second one provides another proof of Lemma 3.

Corollary 9. Let m be an integer, $m \geq 4$. If P_s is an s -PD-set of size $s + 1$ for the binary linear Hadamard code H_m , then any ordering of the elements of P_s gives nested k -PD-sets for $k \in \{1, \dots, s\}$.

Corollary 10. Let m be an integer, $m \geq 4$. If P_s is an s -PD-set of size $s + 1$ for the binary linear Hadamard code H_m , then $s \leq \left\lfloor \frac{2^m - m - 1}{1 + m} \right\rfloor$.

Proof. Following the condition on sets of matrices to be s -PD-sets of size $s + 1$, given by Theorem 5, we have to obtain certain $s + 1$ matrices with no rows in common. Note that the number of possible vectors of length $m + 1$ over \mathbb{Z}_2 with 1 in the first coordinate is 2^m . Thus, taking this fact into account and counting the number of rows of each one of these $s + 1$ matrices, we have that $(s + 1)(m + 1) \leq 2^m$, so $s + 1 \leq \frac{2^m}{m + 1}$ and finally $s \leq \left\lfloor \frac{2^m - m - 1}{1 + m} \right\rfloor$. \square

4 Recursive construction of s -PD-sets for binary linear Hadamard codes

In this section, given an s -PD-set of size l for the binary linear Hadamard code H_m of length 2^m , where $l \geq s + 1$, we show how to construct recursively an s -PD-set of the same size for $H_{m'}$ of length $2^{m'}$ for all $m' > m$.

Given a matrix $M \in \text{PAut}(H_m)$ and an integer $\kappa \geq 1$, we define the matrix $M(\kappa) \in \text{PAut}(H_{m+\kappa})$ as

$$M(\kappa) = \begin{pmatrix} M & \mathbf{0} \\ \mathbf{0} & \text{Id}_\kappa \end{pmatrix}, \quad (5)$$

where Id_κ denotes the $\kappa \times \kappa$ identity matrix.

Proposition 11. *Let m be an integer, $m \geq 4$, and $P_s = \{M_i : 0 \leq i \leq s\}$ be an s -PD-set of size $s+1$ for H_m with information set I_m . Then, $Q_s = \{(M_i^{-1}(\kappa))^{-1} : 0 \leq i \leq s\}$ is an s -PD-set of size $s+1$ for $H_{m+\kappa}$ with information set $I_{m+\kappa}$, for any $\kappa \geq 1$.*

Proof. Since P_s is an s -PD-set for H_m , matrices $(M_1^{-1})^*, \dots, (M_s^{-1})^*$ have no rows in common by Theorem 5. Therefore, it is straightforward to check that matrices $(M_1^{-1}(\kappa))^*, \dots, (M_s^{-1}(\kappa))^*$ have no rows in common either. Moreover, $M_i^{-1}(\kappa) \in \text{PAut}(H_{m+\kappa})$, for all $i \in \{1, \dots, s\}$. Thus, applying again Theorem 5, we have that Q_s is an s -PD-set for $H_{m+\kappa}$. \square

It is important to note that the bound f_{m+1} for H_{m+1} cannot be achieved recursively from an s -PD-set for H_m , since the above recursive construction works for a given fixed s , increasing the length of the Hadamard code.

The above recursive construction only holds when the size of the s -PD-set is exactly $s+1$. Now, we will show a second recursive construction which holds when the size of the s -PD-set is any integer l , $l \geq s+1$. In this case, the elements of $\text{PAut}(H_m)$ will be regarded as permutations of coordinate positions, that is, as elements of $\text{Sym}(2^m)$ instead of matrices of $\text{GL}(m+1, 2)$.

It is well known that a generator matrix G_{m+1} for the binary linear Hadamard code H_{m+1} of length 2^{m+1} can be constructed as follows:

$$G_{m+1} = \begin{pmatrix} G_m & G_m \\ \mathbf{0} & \mathbf{1} \end{pmatrix}, \quad (6)$$

where G_m is a generator matrix for the binary linear Hadamard code H_m of length 2^m . Given two permutations $\sigma_1 \in \text{Sym}(n_1)$ and $\sigma_2 \in \text{Sym}(n_2)$, we define $(\sigma_1 | \sigma_2) \in \text{Sym}(n_1 + n_2)$, where σ_1 acts on the coordinates $\{1, \dots, n_1\}$ and σ_2 on $\{n_1 + 1, \dots, n_1 + n_2\}$.

Proposition 12. *Let m be an integer, $m \geq 4$, and S be an s -PD-set of size l for H_m with information set I . Then, $(S|S) = \{(\sigma|\sigma) : \sigma \in S\}$ is an s -PD-set of size l for H_{m+1} constructed from (6), with any information set $I' = I \cup \{i + 2^m\}$, $i \in I$.*

Proof. Since I is an information set for H_m , we have that $|(H_m)_I| = 2^{m+1}$. Since H_{m+1} is constructed from (6), it follows that $H_{m+1} = \{(x, x), (x, \bar{x}) : x \in H_m\}$, where \bar{x} is the complementary vector of x . A vector and its complementary have different values in each coordinate, so $|(H_{m+1})_{I \cup \{i\}}| = 2^{m+2}$, for all $i \in \{2^m + 1, \dots, 2^{m+1}\}$. Thus, any set of the form $I' = I \cup \{i + 2^m\}$, $i \in I$, is an information set for H_{m+1} .

If $\sigma \in \text{PAut}(H_m)$, then $\sigma(x) = z \in H_m$ for all $x \in H_m$. Therefore, since $(\sigma|\sigma)(x, x) = (z, z)$ and $(\sigma|\sigma)(x, \bar{x}) = (z, z + \sigma(\mathbf{1})) = (z, \bar{z})$, we can conclude that $(\sigma|\sigma) \in \text{PAut}(H_{m+1})$.

Let $e = (a, b) \in \mathbb{Z}_2^{2n}$, where $a = (a_1, \dots, a_n)$, $b = (b_1, \dots, b_n) \in \mathbb{Z}_2^n$, and $n = 2^m$. Finally, we will prove that for every $e \in \mathbb{Z}_2^{2n}$ with $\text{wt}(e) \leq s$, there is $(\sigma|\sigma) \in (S|S)$ such that $(\sigma|\sigma)(e)_{I'} = \mathbf{0}$. Let $c = (c_1, \dots, c_n)$ be the binary vector defined as follows: $c_i = 1$ if and only if $a_i = 1$ or $b_i = 1$, for all $i \in \{1, \dots, n\}$. Note that $\text{wt}(c) \leq s$, since $\text{wt}(e) \leq s$. Taking into account that S is an s -PD-set with respect to I , there is $\sigma \in S$ such that $\sigma(c)_I = \mathbf{0}$. Therefore, we also have that $(\sigma|\sigma)(a, b)_{I \cup J} = \mathbf{0}$, where $J = \{i + n : i \in I\}$. The result follows trivially since $I' \subseteq I \cup J$. \square

5 Finding s -PD-sets of size $s + 1$ for Hadamard \mathbb{Z}_4 -linear codes

For any $m \geq 3$ and each $\delta \in \{1, \dots, \lfloor \frac{m+1}{2} \rfloor\}$, there is a unique (up to equivalence) \mathbb{Z}_4 -linear Hadamard code of length 2^m which is the Gray map image of a quaternary linear code of length $\beta = 2^{m-1}$ and type $2^\gamma 4^\delta$, where $m = \gamma + 2\delta - 1$. Moreover, for a fixed m , all these codes are pairwise nonequivalent, except for $\delta = 1$ and $\delta = 2$, since these ones are equivalent to the binary linear Hadamard code of length 2^m [10]. Therefore, the number of nonequivalent \mathbb{Z}_4 -linear Hadamard codes of length 2^m is $\lfloor \frac{m-1}{2} \rfloor$ for all $m \geq 3$. Note that when $\delta \geq 3$, the \mathbb{Z}_4 -linear Hadamard codes are nonlinear.

Let $\mathcal{H}_{\gamma, \delta}$ be the quaternary linear Hadamard code of length $\beta = 2^{m-1}$ and type $2^\gamma 4^\delta$, where $m = \gamma + 2\delta - 1$, and let $H_{\gamma, \delta} = \Phi(\mathcal{H}_{\gamma, \delta})$ be the corresponding \mathbb{Z}_4 -linear code of length $2\beta = 2^m$. A generator matrix $\mathcal{G}_{\gamma, \delta}$ for the code $\mathcal{H}_{\gamma, \delta}$ can be constructed by using the following recursive constructions:

$$\mathcal{G}_{\gamma+1, \delta} = \begin{pmatrix} \mathcal{G}_{\gamma, \delta} & \mathcal{G}_{\gamma, \delta} \\ \mathbf{0} & \mathbf{2} \end{pmatrix}, \quad (7)$$

$$\mathcal{G}_{\gamma, \delta+1} = \begin{pmatrix} \mathcal{G}_{\gamma, \delta} & \mathcal{G}_{\gamma, \delta} & \mathcal{G}_{\gamma, \delta} & \mathcal{G}_{\gamma, \delta} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix}, \quad (8)$$

starting from $\mathcal{G}_{0,1} = (1)$. We first obtain $\mathcal{G}_{0, \delta}$ from $\mathcal{G}_{0,1}$ by using recursively δ times construction (8). Then, $\mathcal{G}_{\gamma, \delta}$ is managed from $\mathcal{G}_{0, \delta}$ by using γ times construction (7). Note that the rows of order four remain in the upper part of $\mathcal{G}_{\gamma, \delta}$ while those of order two stay in the lower part.

A set $\mathcal{I} = \{i_1, \dots, i_{\gamma+\delta}\} \subseteq \{1, \dots, \beta\}$ of $\gamma + \delta$ coordinate positions is said to be a *quaternary information set* for a quaternary linear code \mathcal{C} of type $2^\gamma 4^\delta$ if $|\mathcal{C}_{\mathcal{I}}| = 2^\gamma 4^\delta$. If the coordinates in \mathcal{I} are ordered in such a way that $|\mathcal{C}_{\{i_1, \dots, i_\delta\}}| = 4^\delta$, it is easy to see that the set $\Phi(\mathcal{I})$, defined as

$$\Phi(\mathcal{I}) = \{2i_1 - 1, 2i_1, \dots, 2i_\delta - 1, 2i_\delta, 2i_{\delta+1} - 1, \dots, 2i_{\delta+\gamma} - 1\},$$

is an information set for $C = \Phi(\mathcal{C})$. For example, the set $\mathcal{I} = \{1\}$ is a quaternary information set for $\mathcal{H}_{0,1}$, so $\Phi(\mathcal{I}) = \{1, 2\}$ is an information set for $H_{0,1} = \Phi(\mathcal{H}_{0,1})$. In general, there is not a unique way to obtain a quaternary information set for the code $\mathcal{H}_{\gamma, \delta}$. The following result provides a recursive and simple form to obtain such a set.

Proposition 13. *Let \mathcal{I} be a quaternary information set for the quaternary linear Hadamard code $\mathcal{H}_{\gamma, \delta}$ of length $\beta = 2^{m-1}$ and type $2^\gamma 4^\delta$, where $m = \gamma + 2\delta - 1$. Then $\mathcal{I} \cup \{\beta + 1\}$ is a quaternary information set for the codes $\mathcal{H}_{\gamma+1, \delta}$ and $\mathcal{H}_{\gamma, \delta+1}$, which are obtained from $\mathcal{H}_{\gamma, \delta}$ by applying (7) and (8), respectively.*

Proof. Since $|\mathcal{H}_{\gamma+1,\delta}| = 2^{\gamma+1}4^\delta$ and $|\mathcal{H}_{\gamma,\delta+1}| = 2^\gamma 4^{\delta+1}$, it is clear that a quaternary information set for codes $\mathcal{H}_{\gamma+1,\delta}$ and $\mathcal{H}_{\gamma,\delta+1}$ should have $\gamma + \delta + 1 = |\mathcal{I}| + 1$ coordinate positions.

Taking into account that $\mathcal{H}_{\gamma,\delta+1}$ is constructed from (8), we have that $\mathcal{H}_{\gamma,\delta+1} = \{(u, u, u, u), (u, u+1, u+2, u+3), (u, u+2, u, u+2), (u, u+3, u+2, u+1) : u \in \mathcal{H}_{\gamma,\delta}\}$. Vectors $u, u+1, u+2$, and $u+3$ have different values in each coordinate, so $|(\mathcal{H}_{\gamma,\delta+1})_{\mathcal{I} \cup \{i\}}| = 2^\gamma 4^{\delta+1}$ for all $i \in \{\beta+1, \dots, 2\beta, 3\beta+1, \dots, 4\beta\}$. In particular, $\mathcal{I} \cup \{\beta+1\}$ is a quaternary information set for $\mathcal{H}_{\gamma,\delta+1}$.

A similar argument holds for $\mathcal{H}_{\gamma+1,\delta}$. Since $\mathcal{H}_{\gamma+1,\delta}$ is constructed from (7), we have that $\mathcal{H}_{\gamma+1,\delta} = \{(u, u), (u, u+2) : u \in \mathcal{H}_{\gamma,\delta}\}$. Vectors u and $u+2$ have different values in each coordinate, so $|(\mathcal{H}_{\gamma+1,\delta})_{\mathcal{I} \cup \{i\}}| = 2^{\gamma+1}4^\delta$ for all $i \in \{\beta+1, \dots, 2\beta\}$. Therefore, $\mathcal{I} \cup \{\beta+1\}$ is a quaternary information set for $\mathcal{H}_{\gamma+1,\delta}$. \square

Despite the fact that the quaternary information set $\mathcal{I} \cup \{\beta+1\}$, given by Proposition 13, is the same for $\mathcal{H}_{\gamma+1,\delta}$ and $\mathcal{H}_{\gamma,\delta+1}$, the information set for the corresponding binary codes $H_{\gamma+1,\delta}$ and $H_{\gamma,\delta+1}$ are $I' = \Phi(\mathcal{I}) \cup \{2\beta+1\}$ and $I'' = \Phi(\mathcal{I}) \cup \{2\beta+1, 2\beta+2\}$, respectively. As for binary linear codes, we can label the i th coordinate position of a quaternary linear code \mathcal{C} , with the i th column of a generator matrix \mathcal{G} of \mathcal{C} . Thus, any quaternary information set \mathcal{I} for \mathcal{C} can also be considered as a set of vectors representing the positions in \mathcal{I} . Then, by Proposition 13, we have that the set $\mathcal{I}_{\gamma,\delta} = \{e_1, e_1 + e_2, \dots, e_1 + e_\delta, e_1 + 2e_{\delta+1}, \dots, e_1 + 2e_{\gamma+\delta}\}$ is a suitable quaternary information set for the code $\mathcal{H}_{\gamma,\delta}$. Depending on the context, $\mathcal{I}_{\gamma,\delta}$ will be considered as a subset of $\{1, \dots, \beta\}$ or as a subset of $\{1\} \times \mathbb{Z}_4^{\delta-1} \times \{0, 2\}^\gamma$.

Example 14. The quaternary linear Hadamard code $\mathcal{H}_{0,3}$ of length 16 can be generated by the matrix

$$\mathcal{G}_{0,3} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \end{pmatrix},$$

obtained by applying two times construction (8) over $\mathcal{G}_{0,1} = (1)$. The set $\mathcal{I}_{0,3} = \{1, 2, 5\}$, or equivalently the set of column vectors $\mathcal{I}_{0,3} = \{(1, 0, 0), (1, 1, 0), (1, 0, 1)\}$ of $\mathcal{G}_{0,3}$, is a quaternary information set for $\mathcal{H}_{0,3}$. By applying constructions (7) and (8) over $\mathcal{G}_{0,3}$, we obtain that matrices

$$\mathcal{G}_{1,3} = \begin{pmatrix} \mathcal{G}_{0,3} & \mathcal{G}_{0,3} \\ \mathbf{0} & \mathbf{2} \end{pmatrix},$$

$$\mathcal{G}_{0,4} = \begin{pmatrix} \mathcal{G}_{0,3} & \mathcal{G}_{0,3} & \mathcal{G}_{0,3} & \mathcal{G}_{0,3} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix},$$

generate the quaternary linear Hadamard codes $\mathcal{H}_{1,3}$ and $\mathcal{H}_{0,4}$ of length 32 and 64, respectively. By Propositions 13, it follows that $\mathcal{I}_{0,3} \cup \{17\} = \{1, 2, 5, 17\}$ is a quaternary information set for $\mathcal{H}_{1,3}$ and $\mathcal{H}_{0,4}$. Despite the fact that the quaternary information set is the same for both codes $\mathcal{H}_{1,3}$ and $\mathcal{H}_{0,4}$, it is important to note that in terms of column vectors representing these positions, we have that $\mathcal{I}_{1,3} = \{(1, 0, 0, 0), (1, 1, 0, 0), (1, 0, 1, 0), (1, 0, 0, 2)\}$ and $\mathcal{I}_{0,4} = \{(1, 0, 0, 0), (1, 1, 0, 0), (1, 0, 1, 0), (1, 0, 0, 1)\}$. Finally, $I' = \Phi(\mathcal{I}_{0,3}) \cup \{33\} = \{1, 2, 3, 4, 9, 10, 33\}$ and $I'' = \Phi(\mathcal{I}_{0,3}) \cup \{33, 34\} = \{1, 2, 3, 4, 9, 10, 33, 34\}$ are information sets for the \mathbb{Z}_4 -linear Hadamard codes $H_{1,3}$ and $H_{0,4}$, respectively.

Let \mathcal{C} be a quaternary linear code of length β and type $2^\gamma 4^\delta$, and let $C = \Phi(\mathcal{C})$ be the corresponding \mathbb{Z}_4 -linear code of length 2β . Let $\Phi : \text{Sym}(\beta) \rightarrow \text{Sym}(2\beta)$ be the map defined as

$$\Phi(\tau)(i) = \begin{cases} 2\tau(i/2), & \text{if } i \text{ is even,} \\ 2\tau((i+1)/2) - 1 & \text{if } i \text{ is odd,} \end{cases}$$

for all $\tau \in \text{Sym}(\beta)$ and $i \in \{1, \dots, 2\beta\}$. Given a subset $\mathcal{S} \subseteq \text{Sym}(\beta)$, we define the set $\Phi(\mathcal{S}) = \{\Phi(\tau) : \tau \in \mathcal{S}\} \subseteq \text{Sym}(2\beta)$. It is easy to see that if $\mathcal{S} \subseteq \text{PAut}(\mathcal{C}) \subseteq \text{Sym}(\beta)$, then $\Phi(\mathcal{S}) \subseteq \text{PAut}(C) \subseteq \text{Sym}(2\beta)$.

Let $\text{GL}(k, \mathbb{Z}_4)$ denote the general linear group of degree k over \mathbb{Z}_4 and let \mathcal{L} be the set consisting of all matrices over \mathbb{Z}_4 of the following form:

$$\begin{pmatrix} 1 & \eta & 2\theta \\ \mathbf{0} & A & 2X \\ \mathbf{0} & Y & B \end{pmatrix},$$

where $A \in \text{GL}(\delta-1, \mathbb{Z}_4)$, $B \in \text{GL}(\gamma, \mathbb{Z}_4)$, X is a matrix over \mathbb{Z}_4 of size $(\delta-1) \times \gamma$, Y is a matrix over \mathbb{Z}_4 of size $\gamma \times (\delta-1)$, $\eta \in \mathbb{Z}_4^{\delta-1}$ and $\theta \in \mathbb{Z}_4^\gamma$.

Lemma 15. *The set \mathcal{L} is a subgroup of $\text{GL}(\gamma + \delta, \mathbb{Z}_4)$.*

Proof. We first need to check that $\mathcal{L} \subseteq \text{GL}(\gamma + \delta, \mathbb{Z}_4)$, in other words, that $\det(\mathcal{M}) \in \{1, 3\}$ (that is, a unit of \mathbb{Z}_4) for all $\mathcal{M} \in \mathcal{L}$. Note that if $\mathcal{M}' \in \text{GL}(k, \mathbb{Z}_4)$, then $\mathcal{M} = \mathcal{M}' + 2\mathcal{R} \in \text{GL}(k, \mathbb{Z}_4)$. Thus, since $\det(\mathcal{M}') \in \{1, 3\}$, we have that $\det(\mathcal{M}) \in \{1, 3\}$, where

$$\mathcal{M}' = \begin{pmatrix} 1 & \eta & \mathbf{0} \\ \mathbf{0} & A & \mathbf{0} \\ \mathbf{0} & Y & B \end{pmatrix}.$$

It is straightforward to check that $\mathcal{M}\mathcal{N} \in \mathcal{L}$ for all $\mathcal{M}, \mathcal{N} \in \mathcal{L}$. □

Let ζ be the map from \mathbb{Z}_4 to \mathbb{Z}_4 which is the usual modulo two map composed with inclusion from \mathbb{Z}_2 to \mathbb{Z}_4 , that is $\zeta(0) = \zeta(2) = 0, \zeta(1) = \zeta(3) = 1$. This map can be extended to matrices over \mathbb{Z}_4 by applying ζ to each one of their entries. Let π be the map from \mathcal{L} to \mathcal{L} defined as

$$\pi(\mathcal{M}) = \begin{pmatrix} 1 & \eta & 2\theta \\ \mathbf{0} & A & 2X \\ \mathbf{0} & \zeta(Y) & \zeta(B) \end{pmatrix},$$

and let $\pi(\mathcal{L}) = \{\pi(\mathcal{M}) : \mathcal{M} \in \mathcal{L}\} \subseteq \text{GL}(\gamma + \delta, \mathbb{Z}_4)$. By Lemma 15, it is clear that $\pi(\mathcal{L})$ is a group with the operation $*$ defined as $\mathcal{M} * \mathcal{N} = \pi(\mathcal{M}\mathcal{N})$ for all $\mathcal{M}, \mathcal{N} \in \pi(\mathcal{L})$. By the proof of Theorem 2 in [9], it is easy to see that the permutation automorphism group $\text{PAut}(\mathcal{H}_{\gamma, \delta})$ of $\mathcal{H}_{\gamma, \delta}$ is isomorphic to $\pi(\mathcal{L})$. Thus, from now on, we identify $\text{PAut}(\mathcal{H}_{\gamma, \delta})$ with this group. Recall that we can label the i th coordinate position of $\mathcal{H}_{\gamma, \delta}$ with the i th column vector w_i of the generator matrix $\mathcal{G}_{\gamma, \delta}$ constructed via (7) and (8), $i \in \{1, \dots, \beta\}$. Therefore, again, any matrix $\mathcal{M} \in \text{PAut}(\mathcal{H}_{\gamma, \delta})$ can be seen as a permutation of coordinate positions $\tau \in \text{Sym}(\beta)$, such that $\tau(i) = j$ as long as $w_j = w_i \mathcal{M}$, $i, j \in \{1, \dots, \beta\}$. For any $\mathcal{M} \in \text{PAut}(\mathcal{H}_{\gamma, \delta})$, we define $\Phi(\mathcal{M}) = \Phi(\tau) \in \text{Sym}(2\beta)$, and for any $\mathcal{P} \subseteq \text{PAut}(\mathcal{H}_{\gamma, \delta})$, we consider $\Phi(\mathcal{P}) = \{\Phi(\mathcal{M}) : \mathcal{M} \in \mathcal{P}\} \subseteq \text{Sym}(2\beta)$.

Lemma 16. Let $\mathcal{H}_{\gamma,\delta}$ be the quaternary linear Hadamard code of length β and type $2^\gamma 4^\delta$ and let $\mathcal{P} \subseteq \text{PAut}(\mathcal{H}_{\gamma,\delta})$. Then, $\Phi(\mathcal{P})$ is an s -PD-set for $H_{\gamma,\delta}$ with information set $\Phi(\mathcal{I}_{\gamma,\delta})$ if and only if for every s -set \mathcal{E} of column vectors of $\mathcal{G}_{\gamma,\delta}$ there is $\mathcal{M} \in \mathcal{P}$ such that $\{g\mathcal{M} : g \in \mathcal{E}\} \cap \mathcal{I}_{\gamma,\delta} = \emptyset$.

Proof. If $\Phi(\mathcal{P})$ is an s -PD-set with respect to the information set $\Phi(\mathcal{I}_{\gamma,\delta})$, then for every s -set $E \subseteq \{1, \dots, 2\beta\}$, there is $\tau \in \mathcal{P} \subseteq \text{Sym}(\beta)$ such that $\Phi(\tau)(E) \cap \Phi(\mathcal{I}_{\gamma,\delta}) = \emptyset$. For every s -set $\mathcal{E} \subseteq \{1, \dots, \beta\}$, let $E_o = \{2i - 1 : i \in \mathcal{E}\}$. We know that there is $\tau \in \mathcal{P}$ such that $\Phi(\tau)(E_o) \cap \Phi(\mathcal{I}_{\gamma,\delta}) = \emptyset$. By the definition of Φ , we also have that $\tau(\mathcal{E}) \cap \mathcal{I}_{\gamma,\delta} = \emptyset$, which is equivalent to the statement.

Conversely, we assume that for every s -set $\mathcal{E} \subseteq \{1, \dots, \beta\}$, there is $\tau \in \mathcal{P} \subseteq \text{Sym}(\beta)$ such that $\tau(\mathcal{E}) \cap \mathcal{I}_{\gamma,\delta} = \emptyset$. For every s -set $E \subseteq \{1, \dots, 2\beta\}$, let \mathcal{E}_o be an s -set such that $\{i : \varphi_1(i) \in E \text{ or } \varphi_2(i) \in E\} \subseteq \mathcal{E}_o$, where $\varphi_1(i) = 2i - 1$ and $\varphi_2(i) = 2i$. Since there is $\tau \in \mathcal{P}$ such that $\tau(\mathcal{E}_o) \cap \mathcal{I}_{\gamma,\delta} = \emptyset$, we have that $\Phi(\tau)(E) \cap \Phi(\mathcal{I}_{\gamma,\delta}) = \emptyset$. \square

Let $\mathcal{M} \in \text{PAut}(\mathcal{H}_{\gamma,\delta})$ and let m_i be the i th row of \mathcal{M} , $i \in \{1, \dots, \delta + \gamma\}$. We define \mathcal{M}^* as the matrix where the first row is m_1 and the i th row is $m_1 + m_i$ for $i \in \{2, \dots, \delta\}$ and $m_1 + 2m_i$ for $i \in \{\delta + 1, \dots, \delta + \gamma\}$.

Theorem 17. Let $\mathcal{H}_{\gamma,\delta}$ be the quaternary linear Hadamard code of type $2^\gamma 4^\delta$. Let $\mathcal{P}_s = \{\mathcal{M}_i : 0 \leq i \leq s\}$ be a set of $s + 1$ matrices in $\text{PAut}(\mathcal{H}_{\gamma,\delta})$. Then, $\Phi(\mathcal{P}_s)$ is an s -PD-set of size $s + 1$ for $H_{\gamma,\delta}$ with information set $\Phi(\mathcal{I}_{\gamma,\delta})$ if and only if no two matrices $(\mathcal{M}_i^{-1})^*$ and $(\mathcal{M}_j^{-1})^*$ for $i \neq j$ have a row in common.

Proof. By Lemma 16 and following a similar argument as in the proof of Theorem 5. \square

Corollary 18. Let \mathcal{P}_s be a set of $s + 1$ matrices in $\text{PAut}(\mathcal{H}_{\gamma,\delta})$. If $\Phi(\mathcal{P}_s)$ is an s -PD-set of size $s + 1$ for $H_{\gamma,\delta}$, then any ordering of elements in $\Phi(\mathcal{P}_s)$ provides nested k -PD-sets for $k \in \{1, \dots, s\}$.

Corollary 19. Let \mathcal{P}_s be a set of $s + 1$ matrices in $\text{PAut}(\mathcal{H}_{\gamma,\delta})$. If $\Phi(\mathcal{P}_s)$ is an s -PD-set of size $s + 1$ for $H_{\gamma,\delta}$, then $s \leq f_{\gamma,\delta}$, where

$$f_{\gamma,\delta} = \left\lfloor \frac{2^{\gamma+2\delta-2} - \gamma - \delta}{\gamma + \delta} \right\rfloor.$$

Proof. Following the condition on sets of matrices to be s -PD-sets of size $s + 1$, given by Theorem 17, we have to obtain certain $s + 1$ matrices with no rows in common. Since the rows of length $\delta + \gamma$ must have 1 in the first coordinate, and elements from $\{0, 2\}$ in the last γ coordinates, the number of possible rows is $4^{\delta-1} 2^\gamma = 2^{\gamma+2\delta-2}$. Thus, taking this fact into account and counting the number of rows of each one of these $s + 1$ matrices, we have that $(s + 1)(\gamma + \delta) \leq 2^{\gamma+2\delta-2}$, and the result follows. \square

We give now an explicit construction of an $f_{0,\delta}$ -PD-set of size $f_{0,\delta} + 1$ for $H_{0,\delta}$. Let $\mathcal{R} = \text{GR}(4^{\delta-1})$ be the Galois extension of dimension $\delta - 1$ over \mathbb{Z}_4 . It is known that \mathcal{R} is isomorphic to $\mathbb{Z}_4[x]/(h(x))$, where $h(x)$ is a monic basic irreducible polynomial of degree $\delta - 1$. Let $f(x) \in \mathbb{Z}_2[x]$ be a primitive polynomial of degree $\delta - 1$. Let $\ell = 2^{\delta-1} - 1$. There is a unique primitive basic irreducible polynomial $h(x)$ dividing $x^\ell - 1$ in $\mathbb{Z}_4[x]$. Let $\mathcal{T} = \{0, 1, \alpha, \dots, \alpha^{\ell-1}\} \subseteq \mathcal{R}$,

where α is a root of $h(x)$. It is well known that any $r \in \mathcal{R}$ can be written uniquely as $r = a + 2b$, where $a, b \in \mathcal{T}$. We take \mathcal{R} as the following ordered set:

$$\begin{aligned}\mathcal{R} &= \{r_1, \dots, r_{4^{\delta-1}}\} \\ &= \{0 + 2 \cdot 0, \dots, \alpha^{\ell-1} + 2 \cdot 0, \dots, 0 + 2 \cdot \alpha^{\ell-1}, \dots, \alpha^{\ell-1} + 2 \cdot \alpha^{\ell-1}\}.\end{aligned}$$

Since $|\mathcal{R}|/\delta = f_{0,\delta} + 1$, we can form $f_{0,\delta} + 1$ disjoint sets of \mathcal{R} of size δ . For all $i \in \{0, \dots, f_{0,\delta}\}$, we consider the $\delta \times \delta$ quaternary matrix

$$\mathcal{N}_i^* = \begin{pmatrix} 1 & r_{\delta i+1} \\ \vdots & \vdots \\ 1 & r_{\delta(i+1)} \end{pmatrix}.$$

Theorem 20. *Let $\mathcal{P}_{f_{0,\delta}} = \{\mathcal{M}_i : 0 \leq i \leq f_{0,\delta}\}$, where $\mathcal{M}_i = \mathcal{N}_i^{-1}$. Then, $\Phi(\mathcal{P}_{f_{0,\delta}})$ is an $f_{0,\delta}$ -PD-set of size $f_{0,\delta} + 1$ for the \mathbb{Z}_4 -linear Hadamard code $H_{0,\delta}$ of length $2^{2\delta-1}$.*

Proof. We need to prove that $r_{\delta i+2} - r_{\delta i+1}, \dots, r_{\delta(i+1)} - r_{\delta i+1}$ are linearly independent over \mathbb{Z}_4 , for all $i \in \{0, \dots, f_{0,\delta}\}$, to guarantee that $\mathcal{N}_i \in \text{PAut}(\mathcal{H}_{0,\delta})$. Note that these vectors are not zero divisors [7]. Since $\alpha^\ell = 1$, $\{r_{\delta i+2} - r_{\delta i+1}, \dots, r_{\delta(i+1)} - r_{\delta i+1}\}$ is one of the following three sets:

$$\begin{aligned}L_1 &= \{1, \dots, \alpha^{\delta-2}\}, \\ L_2 &= \{\alpha^{k+1} - \alpha^k, \dots, \alpha^{k+\delta-1} - \alpha^k\}, \text{ for some } k \in \{0, \dots, \ell-1\}, \\ L_3 &= \{\alpha^{k+1} - \alpha^k, \dots, \alpha^{\ell-1} - \alpha^k, -\alpha^k + 2(b_j - b_i), \alpha^\ell - \alpha^k + 2(b_j - b_i), \dots, \\ &\quad \alpha^{k+\delta-2} - \alpha^k + 2(b_j - b_i)\}, \text{ for some } b_i, b_j \in \mathcal{T} \text{ and } k \in \{0, \dots, \ell-1\}.\end{aligned}$$

Elements in L_1 are clearly linearly independent over \mathbb{Z}_4 . Now we prove that the same property is satisfied in L_2 . Assume on the contrary that there are some $\lambda_i \neq 0$, $i \in \{1, \dots, \delta-1\}$, such that $\sum \lambda_i(\alpha^{k+i} - \alpha^k) = 0$. If $\lambda_i \in \{1, 3\}$ for at least one $i \in \{1, \dots, \delta-1\}$, we get a contradiction. Indeed, if we take modulo 2 in the previous linear combination, we obtain that $\sum \bar{\lambda}_i(\bar{\alpha}^{k+i} - \bar{\alpha}^k) = 0$, where $\bar{\lambda}_i \in \mathbb{Z}_2$ and at least one $\bar{\lambda}_i \neq 0$. This is a contradiction by Lemma 6. On the other hand, if $\lambda_i \in \{0, 2\}$ for all $i \in \{1, \dots, \delta-1\}$ and there is at least one $\lambda_i = 2$, then $\sum 2\lambda'_i(\alpha^{k+i} - \alpha^k) = 2[\sum \lambda'_i(\alpha^{k+i} - \alpha^k)] = 0$, where $\lambda'_i \in \{0, 1\}$ and at least one $\lambda'_i = 1$. Hence, $\sum \lambda'_i(\alpha^{k+i} - \alpha^k) = 2\lambda$ for some $\lambda \in \mathcal{R}$, that is, it is a zero divisor. By taking modulo 2, we obtain a contradiction again by Lemma 6.

We show that elements in $L_3 = \{v_1, \dots, v_{\delta-1}\}$ are also linearly independent over \mathbb{Z}_4 by using a slight modification of the previous argument. Suppose that there is at least one $\lambda_i \neq 0$, $i \in \{1, \dots, \delta-1\}$, such that $\sum \lambda_i v_i = 0$. By taking modulo 2, we obtain that $\bar{\lambda}_{\delta-1}\bar{\alpha}^k + \sum \bar{\lambda}_i(\bar{\alpha}^{k+i} - \bar{\alpha}^k) = \bar{\alpha}^k[\bar{\lambda}_{\delta-1} + \sum \bar{\lambda}_i(\bar{\alpha}^i - 1)] = 0$. Since $\bar{\alpha}^k$ is a unit, it follows that $\bar{\lambda}_{\delta-1} + \sum \bar{\lambda}_i(\bar{\alpha}^i - 1) = 0$, which gives a contradiction if $\lambda_i \in \{1, 3\}$ for at least one index, since $1, \bar{\alpha} - 1, \dots, \bar{\alpha}^{\delta-2} - 1$ are linearly independent over \mathbb{Z}_2 . Note that the binary matrix

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{1} & \text{Id}_{m-1} \end{pmatrix},$$

has determinant 1. If $\lambda_i \in \{0, 2\}$ for all $i \in \{1, \dots, \delta-1\}$, we get a contradiction by applying a similar argument to the one used above.

Finally, by construction, matrices \mathcal{N}_i^* have no rows in common, since their rows are different elements of \mathcal{R} . By Theorem 17, the result follows. \square

Example 21. Let $\mathcal{H}_{0,3}$ be the quaternary linear Hadamard code of length 16 and type $2^0 4^3$. Let $\mathcal{R} = \mathbb{Z}_4[x]/(h(x))$, where $h(x) = x^2 + x + 1$. Note that $h(x)$ is a primitive basic irreducible polynomial dividing $x^3 - 1$ in $\mathbb{Z}_4[x]$. Let α be a root of $h(x)$. Then, $\mathcal{T} = \{0, 1, \alpha, \alpha^2\}$ and elements in \mathcal{R} are ordered as follows:

$$\begin{aligned}\mathcal{R} &= \{r_1, \dots, r_{16}\} \\ &= \{0, 1, \alpha, 3 + 3\alpha, 2, 3, 2 + \alpha, 1 + 3\alpha, 2\alpha, 1 + 2\alpha, \\ &\quad 3\alpha, 3 + \alpha, 2 + 2\alpha, 3 + 2\alpha, 2 + 3\alpha, 1 + \alpha\}.\end{aligned}$$

It is easy to check that matrices $\mathcal{N}_0^* = \text{Id}_3$,

$$\mathcal{N}_1^* = \begin{pmatrix} 1 & 3 & 3 \\ 1 & 2 & 0 \\ 1 & 3 & 0 \end{pmatrix}, \quad \mathcal{N}_2^* = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 1 & 0 & 2 \end{pmatrix}, \quad \mathcal{N}_3^* = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 3 \\ 1 & 3 & 1 \end{pmatrix}, \quad \mathcal{N}_4^* = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix},$$

have no rows in common. Let $\mathcal{P}_4 = \{\mathcal{N}_0^{-1}, \mathcal{N}_1^{-1}, \mathcal{N}_2^{-1}, \mathcal{N}_3^{-1}, \mathcal{N}_4^{-1}\}$, where $\mathcal{N}_0 = \text{Id}_3$,

$$\mathcal{N}_1 = \begin{pmatrix} 1 & 3 & 3 \\ 0 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_2 = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 3 & 2 \\ 0 & 2 & 1 \end{pmatrix}, \quad \mathcal{N}_3 = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 3 & 1 \\ 0 & 2 & 3 \end{pmatrix}, \quad \mathcal{N}_4 = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The set $\Phi(\mathcal{P}_4)$ is a 4-PD-set of size 5 for $H_{0,3}$. Note that the bound $f_5 = 4$ is attained for $H_{0,3}$ despite the search of the 4-PD-set is done in the subgroup $\Phi(\text{PAut}(\mathcal{H}_{0,3})) \leq \text{PAut}(H_{0,3})$, since $f_{0,3} = f_5 = 4$.

We have that the \mathbb{Z}_4 -linear Hadamard code of length 2^m with $\delta = 1$ or $\delta = 2$ is equivalent to the binary linear Hadamard code of length 2^m [10]. However, the technique explained for binary linear Hadamard codes in Section 3 provides better results (in terms of s) than the one explained for \mathbb{Z}_4 -linear Hadamard codes when applied for linear codes, since $f_{\gamma,\delta} \leq f_m$, where $m = \gamma + 2\delta - 1$.

Example 22. We have provided a 2-PD-set of size 3 for the binary linear Hadamard code H_4 of length 16 in Example 8. The code H_4 is equivalent to both \mathbb{Z}_4 -linear Hadamard codes $H_{1,2}$ and $H_{3,1}$. However, a 2-PD-set of size 3 is not achievable for H_4 by using Theorem 17, since $f_{1,2} = f_{3,1} = 1$.

Example 23. The binary linear Hadamard code H_5 of length 32 admits a 4-PD-set of size 5 by Theorem 5, since $f_5 = 4$. Considering H_5 as the Gray map image of the quaternary linear Hadamard code $\mathcal{H}_{2,2}$ or $\mathcal{H}_{4,1}$, no more than a 3-PD-set of size 4 can be found by using Theorem 17, since $f_{4,1} = 2$ and $f_{2,2} = 3$.

6 Recursive construction of s -PD-sets for \mathbb{Z}_4 -linear Hadamard codes

In this section, given an s -PD-set of size l for the \mathbb{Z}_4 -linear Hadamard code $H_{\gamma,\delta}$ of length 2^m and type $2^\gamma 4^\delta$, where $m = \gamma + 2\delta - 1$ and $l \geq s + 1$, we show how to construct recursively an s -PD-set of the same size for $H_{\gamma+i,\delta+j}$ of length 2^{m+i+2j} and type $2^{\gamma+i} 4^{\delta+j}$ for all $i, j \geq 0$.

We first provide a recursive construction considering the elements of $\text{PAut}(\mathcal{H}_{\gamma,\delta})$ as matrices in $\text{GL}(\gamma+\delta, \mathbb{Z}_4)$. This construction can be seen as a natural generalization of the technique introduced for binary linear Hadamard codes in Section 4. Given a matrix $\mathcal{M} \in \text{PAut}(\mathcal{H}_{\gamma,\delta})$ and an integer $\kappa \geq 1$, we define

$$\mathcal{M}(\kappa) = \begin{pmatrix} 1 & \eta & \mathbf{0} & 2\theta \\ \mathbf{0} & A & \mathbf{0} & 2X \\ \mathbf{0} & \mathbf{0} & \text{Id}_\kappa & \mathbf{0} \\ \mathbf{0} & \zeta(Y) & \mathbf{0} & \zeta(B) \end{pmatrix}. \quad (9)$$

Proposition 24. *Let $\mathcal{P}_s = \{\mathcal{M}_0, \dots, \mathcal{M}_s\} \subseteq \text{PAut}(\mathcal{H}_{\gamma,\delta})$ such that $\Phi(\mathcal{P}_s)$ is an s -PD-set of size $s+1$ for $H_{\gamma,\delta}$ with information set $\Phi(\mathcal{I}_{\gamma,\delta})$. Then, $\mathcal{Q}_s = \{(\mathcal{M}_0^{-1}(\kappa))^{-1}, \dots, (\mathcal{M}_s^{-1}(\kappa))^{-1}\} \subseteq \text{PAut}(\mathcal{H}_{\gamma+i,\delta+j})$ and $\Phi(\mathcal{Q}_s)$ is an s -PD-set of size $s+1$ for $H_{\gamma+i,\delta+j}$ with information set $\Phi(\mathcal{I}_{\gamma+i,\delta+j})$, for any $i, j \geq 0$ such that $i+j = \kappa \geq 1$.*

Proof. Note that if $\mathcal{M} \in \text{PAut}(\mathcal{H}_{\gamma,\delta})$, construction (9) provides an element $\mathcal{M}(\kappa) \in \text{GL}(\gamma+\delta+\kappa, \mathbb{Z}_4)$. Taking this into account, together with the fact that Id_κ can split as

$$\text{Id}_\kappa = \begin{pmatrix} \text{Id}_j & \mathbf{0} \\ \mathbf{0} & \text{Id}_i \end{pmatrix},$$

where $i+j = \kappa \geq 1$, it is obvious that $\mathcal{M}^{-1}(\kappa) \in \text{PAut}(\mathcal{H}_{\gamma+i,\delta+j})$ and so its inverse. Thus, $\mathcal{Q}_s \subseteq \text{PAut}(\mathcal{H}_{\gamma+i,\delta+j})$. Finally, repeated rows in matrices $(\mathcal{M}_0^{-1}(\kappa))^*, \dots, (\mathcal{M}_s^{-1}(\kappa))^*$ cannot occur, since this fact implies repeated rows in matrices $(\mathcal{M}_0^{-1})^*, \dots, (\mathcal{M}_s^{-1})^*$ by construction (9). The result follows from Theorem 17. \square

Example 25. *Let $\mathcal{P}_4 = \{\mathcal{M}_0, \dots, \mathcal{M}_4\} \subseteq \text{PAut}(\mathcal{H}_{0,3})$ be the set, given in Example 21, such that $\Phi(\mathcal{P}_4)$ is a 4-PD-set of size 5 for $H_{0,3}$. By Proposition 24, the set $\mathcal{Q}_4 = \{\mathcal{M}_i^{-1}(1))^{-1} : 0 \leq i \leq 4\}$ is contained in both $\text{PAut}(\mathcal{H}_{1,3})$ and $\text{PAut}(\mathcal{H}_{0,4})$. Moreover, $\Phi(\mathcal{Q}_4)$ is a 4-PD-set of size 5 for $H_{1,3}$ and $H_{0,4}$. Nevertheless, it is important to note that the construction of $(\mathcal{M}_i^{-1}(1))^*$ depends on the group where $\mathcal{M}_i^{-1}(1)$ is considered.*

As for binary linear Hadamard codes, a second recursive construction considering the elements of $\text{PAut}(\mathcal{H}_{\gamma,\delta})$ as permutations of coordinate positions, that is as elements of $\text{Sym}(2^m)$, can also be provided. Given four permutations $\sigma_i \in \text{Sym}(n_i)$, $i \in \{1, \dots, 4\}$, we define $(\sigma_1|\sigma_2|\sigma_3|\sigma_4) \in \text{Sym}(n_1+n_2+n_3+n_4)$ in the same way as we defined $(\sigma_1|\sigma_2) \in \text{Sym}(n_1+n_2)$ in Section 4.

Proposition 26. *Let S be an s -PD-set of size l for $H_{\gamma,\delta}$ of length n and type $2^\gamma 4^\delta$ with information set I . Then, $(S|S) = \{(\sigma|\sigma) : \sigma \in S\}$ is an s -PD-set of size l for $H_{\gamma+1,\delta}$ of length $2n$ and type $2^{\gamma+1} 4^\delta$ constructed from (7) and the Gray map, with any information set $I' = I \cup \{i+n\}$, $i \in I$.*

Proof. Since $H_{\gamma+1,\delta} = \{(x, x), (x, \bar{x}) : x \in H_{\gamma,\delta}\}$, where \bar{x} is the complementary vector of x , the result follows using the same argument as in the proof of Proposition 12. By the proof of Proposition 13, we can add any of the coordinate positions of $\{i+n : i \in I\}$ to I in order to form a suitable information set I' for $H_{\gamma+1,\delta}$. \square

Proposition 26 cannot be generalized directly for \mathbb{Z}_4 -linear Hadamard codes $H_{\gamma,\delta+1}$ constructed from (8) and the Gray map. Note that if S is an s -PD-set for $H_{\gamma,\delta}$, then $(S|S|S|S) = \{(\sigma|\sigma|\sigma|\sigma) : \sigma \in S\}$ is not always an s -PD-set for $H_{\gamma,\delta+1}$, since in general $(\sigma|\sigma|\sigma|\sigma) \notin \text{PAut}(H_{\gamma,\delta})$. For example, $\sigma = (1, 5)(2, 8, 3, 6, 4, 7) \in \text{PAut}(H_{0,2}) \subseteq \text{Sym}(8)$, but $\pi = (\sigma|\sigma|\sigma|\sigma) \notin \text{PAut}(H_{0,3}) \subseteq \text{Sym}(32)$, since $\pi(\Phi((0, 0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2, 3, 3, 3, 3))) = \Phi((0, 0, 0, 0, 0, 2, 0, 2, 2, 2, 2, 2, 0, 2, 0, 2, 0, 2, 0, 2, 0, 2, 0, 2)) \notin H_{0,3}$.

Proposition 27. *Let $\mathcal{S} \subseteq \text{PAut}(\mathcal{H}_{\gamma,\delta})$ such that $\Phi(\mathcal{S})$ is an s -PD-set of size l for $H_{\gamma,\delta}$ of length n and type $2^\gamma 4^\delta$ with information set I . Then, $\Phi((\mathcal{S}|S|S|S)) = \{\Phi((\tau|\tau|\tau|\tau)) : \tau \in \mathcal{S}\}$ is an s -PD-set of size l for $H_{\gamma,\delta+1}$ of length $4n$ and type $2^{\gamma+1} 4^{\delta+1}$ constructed from (8) and the Gray map, with any information set $I'' = I \cup \{i+n, j+n\}$, $i, j \in I$ and $i \neq j$.*

Proof. Since $\mathcal{H}_{\gamma,\delta+1}$ is constructed from (8), $\mathcal{H}_{\gamma,\delta+1} = \{(u, u, u, u), (u, u+1, u+2, u+3), (u, u+2, u, u+2), (u, u+3, u, u+1) : u \in \mathcal{H}_{\gamma,\delta}\}$. It is easy to see that if $\tau \in \text{PAut}(\mathcal{H}_{\gamma,\delta})$, then $(\tau|\tau|\tau|\tau) \in \text{PAut}(\mathcal{H}_{\gamma,\delta+1})$.

Let $\sigma = \Phi(\tau)$. Finally, we need to prove that for every $e \in \mathbb{Z}_2^{4n}$ with $\text{wt}(e) \leq s$, there is $(\sigma|\sigma|\sigma|\sigma) \in \Phi((\mathcal{S}|S|S|S))$ such that $(\sigma|\sigma|\sigma|\sigma)(e)_{I''} = \mathbf{0}$, where $I'' \subseteq \{1, \dots, 4n\}$ is an information set for $H_{\gamma,\delta+1}$ with $\gamma+2(\delta+1)$ coordinate positions. Using a similar argument to that given in the proofs of Propositions 12 and 26, the result follows. Moreover, by the proof of Proposition 13, any $I'' = I \cup \{i+n, j+n\}$ with $i, j \in I$ and $i \neq j$ is a suitable information set for $H_{\gamma,\delta+1}$. \square

Propositions 26 and 27 can be applied recursively to acquire s -PD-sets for any \mathbb{Z}_4 -linear Hadamard codes obtained (by using constructions (7) and (8)) from a given \mathbb{Z}_4 -linear Hadamard code where we already have such set. With this aim in mind, let denote by $2S$ the set $(S|S)$ and by $2^i S = 2(2^{i-1} S)$.

Corollary 28. *Let $\mathcal{S} \subseteq \text{PAut}(\mathcal{H}_{\gamma,\delta})$ such that $\Phi(\mathcal{S})$ is an s -PD-set of size l for $H_{\gamma,\delta}$ of length 2^m and type $2^\gamma 4^\delta$ with information set I . Then, $\Phi(2^{i+2j} \mathcal{S})$ is an s -PD-set of size l for $H_{\gamma+i,\delta+j}$ of length 2^{m+i+2j} and type $2^{\gamma+i} 4^{\delta+j}$ with information set obtained by applying recursively Proposition 13, for all $i, j \geq 0$.*

Proof. The result comes trivially by applying Propositions 13, 26 and 27. \square

Note that, from Theorem 20 and Proposition 26, we have explicitly provided an $f_{0,\delta}$ -PD-set of size $f_{0,\delta}+1$ for each nonlinear \mathbb{Z}_4 -linear Hadamard code $H_{\gamma,\delta}$, $\gamma \geq 0, \delta \geq 3$.

7 Conclusions

An alternative permutation decoding method that can be applied to $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes [3], which include \mathbb{Z}_4 -linear codes, was presented in [2]. However, it remained as an open question to determine PD-sets for some families of $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes. In this paper, the problem of finding s -PD-sets of minimum size $s+1$ for binary linear and \mathbb{Z}_4 -linear Hadamard codes is addressed by finding $s+1$ invertible matrices over \mathbb{Z}_2 or \mathbb{Z}_4 , respectively, which satisfy certain conditions. Moreover, note that the first examples and constructions of (nonlinear) \mathbb{Z}_4 -linear Hadamard codes are provided. This approach establishes equivalent results to the ones obtained for simplex codes in [4].

As a future research in this topic, it would be interesting to provide explicitly an $f_{\gamma,\delta}$ -PD-set of size $f_{\gamma,\delta} + 1$ for $H_{\gamma,\delta}$, s -PD-sets of minimum size for $\mathbb{Z}_2\mathbb{Z}_4$ -linear Hadamard codes in general [13], or other families of \mathbb{Z}_4 -linear codes such as Kerdock codes [7].

References

- [1] R. Barrolleta and M. Villanueva, “Partial permutation decoding for binary linear Hadamard codes,” *Electron. Note Discr. Math.* **46**, 35–42 (2014).
- [2] J. J. Bernal, J. Borges, C. Fernández-Córdoba, and M. Villanueva, “Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes,” *Des. Codes and Cryptogr.* **76**(2), 269–277 (2015).
- [3] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, “ $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: generator matrices and duality,” *Des. Codes and Cryptogr.* **54**, 167–179 (2010).
- [4] W. Fish, J. D. Key, and E. Mwambene, “Partial permutation decoding for simplex codes,” *Adv. Math. Commun.* **6**(4), 505–516 (2012).
- [5] D. M. Gordon, “Minimal permutation sets for decoding the binary Golay codes,” *IEEE Trans. Inf. Theory* **28**(3), 541–543 (1982).
- [6] W. C. Huffman, *Codes and groups, Handbook of coding theory*, eds. V. S. Pless and W. C. Huffman, Elsevier (1998).
- [7] A. R. Hammons, Jr, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, “The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals, and related codes,” *IEEE Trans. Inf. Theory* **40**(2), 301–319, (1994).
- [8] H.-J. Kroll and R. Vicenti, “PD-sets for binary RM-codes and the codes related to the Klein quadric and to the Schubert variety of $\text{PG}(5,2)$,” *Discrete Math.* **308**, 408–414, (2008).
- [9] D. S. Krotov and M. Villanueva, “Classification of the $\mathbb{Z}_2\mathbb{Z}_4$ -linear Hadamard codes and their automorphism groups,” *IEEE Trans. Inf. Theory* **61**(2), 887–894 (2015).
- [10] D. S. Krotov, “ \mathbb{Z}_4 -linear Hadamard and extended perfect codes,” *Electron. Note Discr. Math.* **6**, 107–112 (2001).
- [11] F. J. MacWilliams, “Permutation decoding of systematic codes,” *Bell System Tech. J.* **43**, 485–505 (1964).
- [12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company (1977).
- [13] K.T. Phelps, J. Rifà, and M. Villanueva, “On the additive \mathbb{Z}_4 -linear and non- \mathbb{Z}_4 -linear Hadamard codes. Rank and Kernel,” *IEEE Trans. on Information Theory* **52**(1), 316–319 (2005).

- [14] J. Pernas, J. Pujol, and M. Villanueva, “Characterization of the automorphism group of quaternary linear Hadamard codes,” *Des. Codes Cryptogr.* **70**(1-2), 105–115 (2014).
- [15] P. Seneviratne, “Partial permutation decoding for the first-order Reed-Muller codes,” *Discrete Math.* **309**(8), 1967–1970 (2009).
- [16] J. Wolfmann, “A permutation decoding of the (24,12,9) Golay code,” *IEEE Trans. on Information Theory* **29**(5), 748–750 (1983).